Facultad de Informática
Grado en Ingeniería Informática

Lógica

PARTE 4: RESOLUCIÓN

Tema 14: Sustitución y Unificación

Profesor: Javier Bajo
jbajo@fi.upm.es

Introducción.

❑ Componentes

Parte 1
Lógica Proposicional

Parte 2
Lógica de Primer Orden

Parte 3
Demostración Automática

Parte 4
Resolución

Sustitución.

- **Sustitución:** Una *sustitución* es una función finita de un conjunto de variables de un lenguaje en el de términos. Se representa como $\alpha = \{x_1/t_1, x_2/t_2, \ldots, x_n/t_n\}$ donde $x_1, \ldots, x_n$ son variables diferentes y $t_1, \ldots, t_n$ son términos tales que, en cada t_i no aparece la variable x_i
- Un par x_i/t_i se denomina *ligadura*
- Una sustitución que no sustituye ninguna variable se llama *sustitución vacía (λ)*
- Una sustitución que sustituye variables por otras variables se denomina *renombrado*
- *Dominio(α)* $= \{x_i \,/\, x_i/t_i \in \alpha\}$
- *Rango(α)* $= \{y_i \,/\, y_i$ aparece en t_i y $x_i/t_i \in \alpha\}$

Ejemplos: Ctes = {a, b, c, d}, Var = {x, y, z, w}, Func = {f/1, h/2}

$\alpha 1 = \{x/f(a), y/x, z/h(b,y), w/a\}$	Dominio(α1) = {x, y, z, w}	Rango(α1) = {x, y}
$\alpha 2 = \{x/a, y/a, z/h(b,c), w/f(d)\}$	Dominio(α2) = {x, y, z, w}	Rango(α2) = $\varnothing$
$\alpha 3 = \{x/y, z/w\}$ (renombrado)	Dominio(α3) = {x, z}	Rango(α3) = {y, w}
$\lambda = \{x/x, y/y, z/z\}$		

Sustitución.

- Dada una fórmula F y una sustitución $\alpha = \{x_1/t_1, \ldots, x_n/t_n\}$, se denomina *aplicación de α a F, (Fα)* a la fórmula obtenida reemplazando ***simultáneamente*** cada ocurrencia en F de x_i por t_i, para cada $x_i/t_i \in \alpha$.

  α = {x/f(a), y/x, z/h(b,y), w/a}

  P(x, y, z) α = P(f(a), f(a), h(b,f(a))) *incorrecto*

  P(x, y, z) α = P(f(a), x, h(b,y)) *correcto*

- Una fórmula F' es *instancia* de otra fórmula F si existe una sustitución no vacía α tal que F' = Fα

- Una sustitución α es *idempotente* si Dominio(α) $\cap$ Rango(α) = $\varnothing$

- Si α es una sustitución idempotente entonces (Fα)α = Fα

  α1 = {x/a, y/f(b), z/v} P(x, y, w, z) α1 = P(a, f(b), w, v)

  P(a, f(b), w, v) α1 = P(a, f(b), w, v)

  α2 = {x/a, y/f(b), z/x} P(x, y, w, z) α2 = P(a, f(b), w, x)

  P(a, f(b), w, x) α2 = P(a, f(b), w, a)

  α1 es idempotente, α2 no

Sustitución.

- Dadas dos sustituciones $\alpha = \{x_1/t_1, \ldots, x_n/t_n\}$ y $\beta = \{y_1/s_1, \ldots, y_m/s_m\}$ su *composición* $\alpha\beta$ se define eliminando del conjunto

$$\{x_1/t_1\beta, \ldots, x_n/t_n\beta, y_1/s_1, \ldots, y_m/s_m\}$$

  las ligaduras $x_i/t_i\beta$ tales que $x_i \equiv t_i\beta$,

  y las ligaduras y_i/s_i tales que $y_i \in \{x_1,\ldots,x_n\}$

- Ejemplo:

  si $\alpha = \{x/3, y/f(x,1)\}$ y $\beta = \{x/4\}$

  entonces $\alpha\beta = \{x/3, y/f(4,1)\}$ y

  $\beta\alpha = \{x/4, y/f(x,1)\}$

- Propiedades de la composición:

  $(F\alpha)\beta = F(\alpha\beta)$

  $(\alpha\beta)\gamma = \alpha(\beta\gamma)$

  $\alpha\lambda = \lambda\alpha = \alpha$

  $\alpha\beta \neq \beta\alpha$

Unificación.

- Una sustitución α es un *unificador* de dos fórmulas A y B si $A\alpha = B\alpha$. En este caso se dice que A y B son unificables. Informalmente, unificar es el proceso por el cual dos o mas expresiones se convierten en idénticas mediante una sustitución: la sustitución unificadora.
- Un unificador α de A y B se denomina *unificador de máxima generalidad (umg)* sii para cualquier otro unificador β de A y B existe alguna sustitución γ tal que $\beta=\alpha\gamma$
- Si dos fórmulas son unificables entonces tienen umg
- El umg de dos fórmulas es único (salvo renombrado)
- Ejemplo:

  $A \equiv P(x, f(x, g(y)), z)$ y $B \equiv P(r, f(r, u), a)$

  $\alpha 1 = \{x/r, u/g(y), z/a\}$ y $\alpha 2 = \{x/a, r/a, y/b, u/g(b), z/a\}$

  $A\alpha 1 = B\alpha 1 = P(r, f(r, g(y)), a)$

  $A\alpha 2 = B\alpha 2 = P(a, f(a, g(b)), a)$

  $\alpha 1$ y $\alpha 2$ son unificadores de A y B, pero $\alpha 1$ es el umg de A y B

  $\gamma = \{r/a, y/b\}$, $\alpha 2 = \alpha 1\ \gamma$

Unificación.

Algoritmo de Unificación:

Sean A y B dos átomos con el mismo símbolo de predicado:

(1) $\alpha = \lambda$

(2) Mientras $A\alpha \neq B\alpha$:

(2.1) Encontrar el símbolo más a la izquierda en $A\alpha$ tal que el símbolo correspondiente en $B\alpha$ sea diferente

(2.2) Sean t_A y t_B los términos de $A\alpha$ y $B\alpha$ que empiezan con esos símbolos:

(a) Si ni t_A ni t_B son variables o, si uno de ellos es una variable que aparece en el otro ➔ terminar con fallo (A y B no son unificables)

(b) En otro caso, sea t_A una variable ➔ el nuevo α es el resultado de $\alpha\{t_A/t_B\}$

(3) Terminar, siendo α el umg de A y B

Unificación.

- **Algoritmo de Unificación:**

Ejemplo: A ≡ P(x, x) y B ≡ P(f(a), f(b))

α	A α	B α	(t_A, t_B)
λ	P(x, x)	P(f(a), f(b))	(x,f(a))
{x/f(a)}	P(f(a), f(a))	P(f(a), f(b))	(a,b)

Fallo ➔ A y B no son unificables

Ejemplo: A ≡ P(x, f(y)) y B ≡ P(z, x)

α	A α	B α	(t_A, t_B)
λ	P(x, f(y))	P(z, x)	(x,z)
{x/z}	P(z, f(y))	P(z, z)	(f(y),z)
{x/f(y), z/f(y)}	P(f(y), f(y))	P(f(y), f(y))	

➔ A y B son unificables y su umg es {x/f(y), z/f(y)}

Resolución con Variables.

- **Regla de resolución con umg:** Sean $L_1 \vee \ldots \vee L_n \vee C_1$ y $\neg L_1' \vee \ldots \vee \neg L_m' \vee C_2$ dos cláusulas, donde todos los L_{ij} son literales con el mismo símbolo de predicado. Puede deducirse una nueva cláusula $(C_1 \rho_1 \vee C_2 \rho_2)\beta$, llamada *resolvente*, donde
  - ρ_1 y ρ_2 son renombrados cuyos dominios respectivos son todas las variables de cada cláusula y $\text{Rango}(\rho_1) \cap \text{Rango}(\rho_2) = \varnothing$
  - β es umg de $\{L_1 \rho_1, \ldots, L_n \rho_1, L_1'\rho_2, \ldots, L_m'\rho_2\}$

- La regla de resolución con umg se apoya en una versión de la **regla de factorización** para LPO: Dada una cláusula $L_1 \vee \ldots \vee L_n \vee C$, siendo $L_1, \ldots, L_n$ literales con el mismo símbolo de predicado, puede deducirse una nueva cláusula $L \vee C\beta$ donde
  - β es unificador de $L_1, \ldots, L_n$
  - $L = L_1\beta = \ldots = L_n\beta$

  El literal L se denomina *factor* de $L_1 \vee \ldots \vee L_n \vee C$

Resolución con Variables.

- La regla de resolución con umg es correcta

  Si por su aplicación deducimos □, entonces el conjunto inicial de cláusulas es insatisfacible *(demostración en el anexo al final del tema).*

- La regla de resolución con umg es completa

  Si el conjunto inicial es insatisfacible, entonces podemos asegurar que con la aplicación sucesiva de la regla de resolución llegaremos a deducir la cláusula vacía *(demostración en el anexo al final del tema).*

- **Un conjunto de cláusulas es insatisfacible sii se puede deducir □ a partir de él por resolución con umg** *(demostración en el anexo al final del tema).*

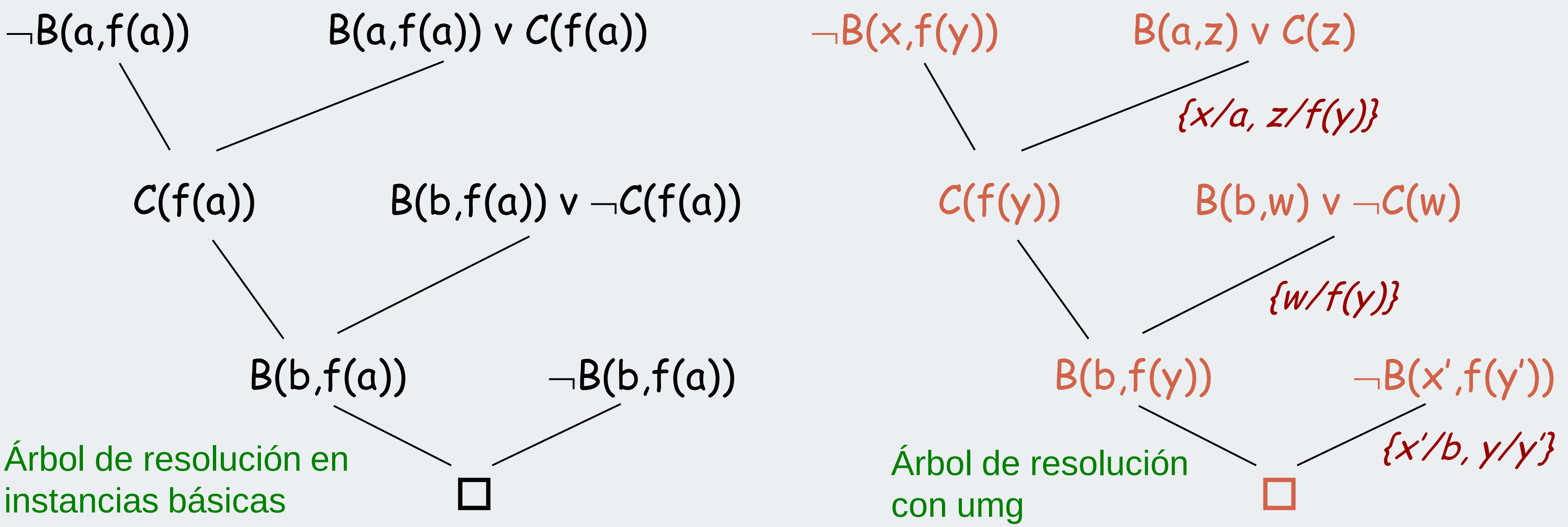
- Por tanto, **el método general de insatisfacibilidad se puede reducir a la búsqueda de □** a partir del conjunto de cláusulas, en lugar de tener que generar conjuntos de instancias básicas

Resolución con Variables.

- Pueden construirse árboles de resolución en los que los resolventes de cada dos cláusulas se obtienen en un paso de resolución con umg
- Por cada paso de resolución en instancias básicas puede definirse un paso de resolución con umg

Ejemplo: C_1: ¬B(x,f(y)) C_2: B(a,z) v C(z) C_3: B(b,w) v ¬C(w)

I_1: ¬B(a,f(a)) I_1': ¬B(b,f(a)) I_2: B(a,f(a)) v C(f(a)) I_3: B(b,f(a)) v ¬C(f(a))



Procedimiento de Saturación.

- **Procedimiento de saturación:** Sea C un conjunto de cláusulas
  1) Sea $S_0 = C$ y $n = 0$
  2) Si $\square \in S_n$ ➔ C es insatisfacible
  3) Construir S_{n+1} = {resolventes de C1 y C2 / C1 $\in (S_0 \cup \ldots \cup S_n)$, C2 $\in S_n$}
  4) Si $S_{n+1} = \emptyset$ o $S_{n+1} \subset S_0 \cup \ldots \cup S_n$ ➔ C es satisfacible
  5) Hacer $n = n+1$ y repetir desde 2)

- El paso 3) requiere considerar todos los posibles factores F, de predicados distintos, de las cláusulas C1 y C2 sobre los que se pueden resolver ambas cláusulas con el umg que da F

- Este procedimiento genera *todos* y *sólo* los resolventes posibles a partir de un conjunto de cláusulas

- Este procedimiento es completo: Un conjunto de cláusulas C es insatisfacible sii el procedimiento de saturación encuentra $\square$ a partir de C

Procedimiento de Saturación.

S_0:

1) $P \vee Q$
2) $\neg P \vee Q$
3) $P \vee \neg Q$
4) $\neg P \vee \neg Q$

S_1:

5)	Q	de 1) y 2)
6)	P	de 1) y 3)
7)	$Q \vee \neg Q$	de 1) y 4)
8)	$P \vee \neg P$	de 1) y 4)
9)	$Q \vee \neg Q$	de 2) y 3)
10)	$P \vee \neg P$	de 2) y 3)
11)	$\neg P$	de 2) y 4)
12)	$\neg Q$	de 3) y 4)

S_2:

13)	$P \vee Q$	de 1) y 7)
14)	$P \vee Q$	de 1) y 8)
15)	$P \vee Q$	de 1) y 9)
16)	$P \vee Q$	de 1) y 10)
17)	Q	de 1) y 11)
18)	P	de 1) y 12)
19)	Q	de 2) y 6)
20)	$\neg P \vee Q$	de 2) y 7)
21)	$\neg P \vee Q$	de 2) y 8)
22)	$\neg P \vee Q$	de 2) y 9)
23)	$\neg P \vee Q$	de 2) y 10)
24)	$\neg P$	de 2) y 12)
25)	P	de 3) y 5)
26)	$P \vee \neg Q$	de 3) y 7)
27)	$P \vee \neg Q$	de 3) y 8)
28)	$P \vee \neg Q$	de 3) y 9)
29)	$P \vee \neg Q$	de 3) y 10)
30)	$\neg Q$	de 3) y 11)
31)	$\neg P$	de 4) y 5)
32)	$\neg Q$	de 4) y 6)
33)	$\neg P \vee \neg Q$	de 4) y 7)
34)	$\neg P \vee \neg Q$	de 4) y 8)
35)	$\neg P \vee \neg Q$	de 4) y 9)
36)	$\neg P \vee \neg Q$	de 4) y 10)
37)	Q	de 5) y 7)
38)	Q	de 5) y 9)
39)	$\square$	de 5) y 12)

Se generan muchas cláusulas redundantes e irrelevantes:

- 7), 8), 9) y 10) son tautologías
- Su interacción con otras genera más cláusulas redundantes
- P, Q, $\neg$P y $\neg$Q se generan repetidas veces

En realidad bastaría con generar las cláusulas 5), 12) y 39)

Anexo: Corrección de la resolución con umg.

- Corrección de la regla de resolución con umg: La estructura deductiva $[\forall x_1 \ldots x_p(L_1 \vee \ldots \vee L_n \vee C_1), \forall y_1 \ldots y_q(\neg L_1' \vee \ldots \vee \neg L_m' \vee C_2)] \vdash \forall z_1 \ldots z_r(C_1\rho_1 \vee C_2\rho_2)\beta$ es correcta
  - siendo $x_1 \ldots x_p$, $y_1 \ldots y_q$ y $z_1 \ldots z_r$ todas las variables de las respectivas cláusulas
  - ρ_1 y ρ_2 renombrados de $x_1 \ldots x_p$ y $y_1 \ldots y_q$ respectivamente y
  - β es umg de $\{L_1\rho_1, \ldots, L_n\rho_1, L_1'\rho_2, \ldots, L_m\rho_2\}$

Demostración:

1. $\forall x_1 \ldots x_p(L_1 \vee \ldots \vee L_n \vee C_1)$ Hipótesis
2. $\forall y_1 \ldots y_q(\neg L_1' \vee \ldots \vee \neg L_m' \vee C_2)$ Hipótesis
3. $F \vee ..n.. \vee F \vee E_1$ Sustitución u_i/t_i tal que $L_i = L_j$ y renombrado de variables
4. $\neg F \vee ..m.. \vee \neg F \vee E_2$ Sustitución v_i/t_i tal que $L_i' = L_j'$ y renombrado de variables
5. $F \vee E_1$ Intercambio $F \vee F$ por F (Idempotencia) (n-1 veces)
6. $\neg F \vee E_2$ Intercambio $\neg F \vee \neg F$ por $\neg F$ (Idempotencia) (m-1 veces)
7. $E_1 \vee E_2$ Corte
8. $\forall z_1 \ldots z_r(C_1 \vee C_2)$ Generalización

Anexo: Corrección de la resolución con umg I.

- Lema de elevación: Si B es resolvente de B_1 y B_2, ambas instancias básicas de C_1 y C_2, respectivamente, entonces
  - Existe una cláusula C tal que B es instancia básica suya
  - C resulta de un paso de resolución entre *copias* de C_1 y C_2 sobre un literal L, factor común a ambas: $C_1 = L_1$ v...v L_n v D_1, $C_2 = \neg L_1'$v...v $\neg L_m'$ v D_2, C = $(D_1\rho_1$ v $D_2\rho_2)\theta$, tal que ρ_1 y ρ_2 son renombrados y θ es un umg: $\{L_1\rho_1 \ldots L_n\rho_1\}\theta = \{L_1'\rho_2 \ldots L_m'\rho_2\}\theta = L$

- Demostración:
  1. Existen B_1= F v ...v F v E_1 y B_2= ¬F v ...v ¬F v E_2 tal que B = E_1 v E_2
  2. Existen σ_1, σ_2, Rango(σ_1)=Rango(σ_2)=∅ (e.d. sin variables) tal que: $C_1\sigma_1 = B_1$ y $C_2\sigma_2 = B_2$
  3. Existen σ_1' y ρ_1, tal que $C_1\rho_1\sigma_1' = C_1\sigma_1$ y ρ_1 es un renombrado de todas las variables de C_1
  4. Existen σ_2' y ρ_2, tal que $C_2\rho_2\sigma_2' = C_2\sigma_2$ y ρ_2 es un renombrado de todas las variables de C_2 sin variables compartidas con ρ_1 (e.d. Rango(ρ_2) ∩ Rango(ρ_1)=∅)
  5. $C_1\rho_1\sigma_1' = C_1\rho_1(\sigma_1'\sigma_2')$, pues $C_1\rho_1(\sigma_1'\sigma_2') = C_1(\rho_1\sigma_1')\sigma_2'$ (asociatividad) = $C_1\rho_1\sigma_1'$, dado que Rango(σ_1')=∅ (las ligaduras de σ_2' son irrelevantes)
  6. $C_2\rho_2\sigma_2' = C_2\rho_2(\sigma_1'\sigma_2')$, pues $C_2\rho_2(\sigma_1'\sigma_2') = C_2(\rho_2\sigma_1')\sigma_2' = (C_2\rho_2\sigma_1')\sigma_2'$ y $C_2\rho_2\sigma_1' = C_2\rho_2$, pues Rango($\rho_2$) ∩ Rango($\rho_1$)=∅ y Dominio($\sigma_1'$)=Rango($\rho_1$) (las ligaduras de σ_1' son irrelevantes)
  7. Sea $\sigma = \sigma_1'\sigma_2'$, σ es una sustitución básica pues σ_1 y σ_2 lo son

Anexo: Corrección de la resolución con umg II.

- Demostración del lema de elevación (continuación):

8. $B_1=C_1\rho_1\sigma=(L_1 v...v\ L_n\ v\ D_1)\rho_1\sigma=L_1\rho_1\sigma\ v...v\ L_n\rho_1\sigma\ v\ D_1\rho_1\sigma=F\ v\ ...v\ F\ v\ E_1$ y $B_2=C_2\rho_2\sigma=(\neg L_1' v...v\ \neg L_m'\ v\ D_2)\rho_2\sigma=\ \neg L_1'\rho_2\sigma\ v...v\ \neg L_m'\rho_2\sigma\ v\ D_2\rho_2\sigma=\ \neg F\ v...v\ \neg F\ v\ E_2$
9. $\{L_1\rho_1,...,L_n\rho_1\}\sigma = F$ y $\{\neg L_1'\rho_2,...,\neg L_m'\rho_2\}\sigma = \neg F$, luego $\{L_1\rho_1,...,L_n\rho_1,L_1'\rho_2,...,L_m'\rho_2\}\sigma=F$
10. Si $\{L_1\rho_1,...,L_n\rho_1,L_1'\rho_2,...,L_m'\rho_2\}$ es unificable, existe un umg θ para este conjunto
11. Sea $L = \{L_1\rho_1,...,L_n\rho_1,L_1'\rho_2,...,L_m'\rho_2\}\theta$, luego L es factor de $C_1\rho_1$ y $C_2\rho_2$
12. Si θ es umg y σ un unificador cualquiera, existe ω tal que $\theta \circ \omega = \sigma$
13. $B = E_1\ v\ E_2 = D_1\rho_1\sigma\ v\ D_2\rho_2\sigma = (D_1\rho_1\ v\ D_2\rho_2)\sigma = (D_1\rho_1\ v\ D_2\rho_2)\theta\omega$
14. Sea $C = (D_1\rho_1\ v\ D_2\rho_2)\theta$, entonces $B = C\omega$ y $C\omega$ es instancia básica de C pues $\theta \circ \omega = \sigma$ y σ es una sustitución básica.

Anexo: Corrección de la resolución con umg III.

- Lema: Si un conjunto C de cláusulas es insatisfacible, se deduce de él □ por resolución con umg

1. Si C es insatisfacible, entonces de un conjunto de instancias básicas suyo se deduce □ por resolución
2. Existe un árbol de resolución de □ con profundidad n
3. Si n=1 la resolución entre instancias básicas permite definir un paso de resolución con umg entre cláusulas de C (Lema de elevación)
4. Si n>1, existe un conjunto de resolventes R de cláusulas de C, tal que C ∪ R tiene un árbol de resolución de □ con profundidad n-1:
   - Para cada paso de resolución de nivel 1, sean B_1 y B_2 instancias básicas de cláusulas C_1 y C_2 de C las que se resuelven dando B
   - Existe un paso de resolución con umg entre C_1 y C_2 con resolvente RC tal que B es instancia básica de RC (Lema de elevación). Sea R el conjunto de dichas cláusulas RC.
   - Si se eliminan todos los pasos de resolución que dan instancias B, los nuevos nodos de nivel 0 serán instancias básicas de R o de C.
   - El conjunto C ∪ R tiene un árbol de resolución de □ con profundidad n-1
5. Para el nuevo conjunto C′ = C ∪ R, si n-1=1 se deduce □ por resolución con umg (por 3). Si n-1>1, existe un conjunto de resolventes R′ de cláusulas de C′, tal que C′ ∪ R′ tiene un árbol de resolución de □ con profundidad n-2

   Y así sucesivamente. Por tanto:
6. Del conjunto C se puede deducir □ por resolución con umg

Anexo: Corrección de la resolución con umg IV.

- Teorema: Un conjunto de cláusulas es insatisfacible sii se deduce de él □ por resolución con umg

$\Rightarrow$ Si el conjunto de cláusulas es insatisfacible entonces se deduce de él □ por resolución con umg (lema anterior)

$\Leftarrow$ 1. C |— □ aplicando la regla de resolución con umg

2. La regla de resolución con umg es una regla correcta de deducción, luego si C |— □ entonces C |= □ (teorema de validez)

3. □ es falsa en cualquier interpretación

4. C no puede ser verdadero en ninguna interpretación

5. C es insatisfacible